ACUERDO QUE EMITE EL COMITÉ DE CONTROL INTERNO DE LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN, POR MEDIO DEL CUAL SE ESTABLECEN LAS POLÍTICAS PARA EL USO DE EQUIPOS INFORMÁTICOS, INTERNET, PROGRAMAS ELECTRÓNICOS Y UNIDADES DE ALMACENAMIENTO DE LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIPON

CONSIDERANDO

PRIMERO. Que el artículo 109 ter de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo, instituye al Sistema Estatal Anticorrupción como la instancia de coordinación entre las autoridades de todos los órdenes de gobierno en la entidad, competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos. Asimismo, le atribuye al Comité Coordinador de este Sistema, entre otras atribuciones, la operación de mecanismos de coordinación con el sistema federal y la aplicación de los que en estas materias generen las instituciones competentes estales y municipales en los términos que determine el Sistema Nacional.

SEGUNDO. Que de conformidad al artículo 8, fracciones X y XI, de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo, el Comité Coordinador del mencionado Sistema, tiene entre otras facultades, determinar los mecanismos de suministro, intercambio, sistematización y actualización de la información que sobre las materias relacionadas con el Sistema Estatal generen los Órganos del Estado; así como proporcionar datos e información a la Plataforma Digital Estatal para su manejo.

TERCERO. Que el artículo 47 de la Ley en cita, señala que el Comité Coordinador del Sistema Estatal Anticorrupción, implementará la Plataforma Digital Estatal, con apego a los lineamientos señalados por la Federación, que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en dicha Ley y en la Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo, así como para los sujetos de la referida Ley del Sistema, atendiendo a las necesidades de accesibilidad de los usuarios. También dispone que el Comité Coordinador será el responsable de proporcionar la información necesaria al Comité Coordinador del Sistema Nacional Anticorrupción, para que sea integrada a la Plataforma Digital Nacional.

CUARTO. Que el artículo 48, fracción III, de la Ley referida con anterioridad, establece que la Plataforma Digital del Sistema Estatal, estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Estatal y contará, con los siguientes sistemas electrónicos:

I. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;

II. Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas;

III. Sistema de servidores públicos y particulares sancionados;

IV. Sistema de información y comunicación con el Sistema Nacional y con el Sistema Nacional de Fiscalización;

V. Sistema de denuncia pública de faltas administrativas y hechos de corrupción; y,

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

VI. Sistema de Información Pública de Contrataciones.

QUINTO. Que la Plataforma Digital Estatal será administrada por la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, según lo establecen los numerales 49, en correlación con el 37, fracción X, y 12 de las Bases para el funcionamiento de la Plataforma Digital Estatal.

En ese sentido, el artículo 6 de la Bases antes citadas, dispone que, para el correcto funcionamiento de cada uno de los Sistemas, la Secretaría Ejecutiva emitirá los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir las Bases.

Asimismo, el artículo 19 de la Bases antes citadas, dispone que, para el acceso restringido de la información, la Secretaría Ejecutiva establecerá los mecanismos de seguridad necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.

SEXTO. Que con fecha 15 de diciembre de 2021 se declaró el inicio de operación del Sistema de los Servidores Públicos que Intervengan en Procedimientos de Contrataciones Públicas, Sistema de Servidores Públicos y Particulares Sancionados ,y los datos que los Órganos del Estado incorporen a estos Sistemas se encontrarán almacenados en el equipo servidor de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

SÉPTIMO. Que derivado del análisis de vulnerabilidades realizado el 29 de diciembre de 2021 y de la Matriz para la Administración de Riesgos de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, aprobada por el Comité de Control Interno de la misma Secretaría el 31 de mayo de 2022, se determinó la pertinencia de la emisión de políticas para su implementación al interior de la propia Secretaría Ejecutiva, con el objetivo de garantizar la seguridad de los datos almacenados en los equipos informáticos de la Secretaría Ejecutiva; asegurar su confidencialidad, integridad, así como la disponibilidad y activos de información; además de garantizar el buen uso y manejo de los bienes informáticos para su óptima funcionalidad y rendimiento.

Por lo anterior, y con fundamento en los artículos 37, fracción X; 47 y 48 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo; 19, 31, 32, 33, 34, 35 y 36 de las Bases para el Funcionamiento de la Plataforma Digital Estatal; Artículos 18, fracción XIV y XVIII.; 28 fracción VI, XV; 30 fracción I, V, VIII, X, XI y XXI del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, se emiten las siguientes:

POLÍTICAS PARA EL USO DE EQUIPOS INFORMÁTICOS, INTERNET, PROGRAMAS ELECTRÓNICOS, UNIDADES DE ALMACENAMIENTO DE LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN

Del Objetivo. Las presentes Políticas tienen como objetivo:

a) Apoyar a la seguridad de los datos que se encuentran almacenados en el equipo servidor de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, que alberga la Plataforma Digital Estatal;

asegurar la confidencialidad, integridad, disponibilidad de la información y activos de información que se encuentran en el mismo;

b) El resguardo y preservación de los equipos informáticos de la Secretaría Ejecutiva;
c) Asegurar el buen uso y manejo de todos los bienes y equipos informáticos de la Secretaría Ejecutiva para su óptimo funcionamiento y rendimiento.

Del alcance: Servicios, datos e información, aplicaciones software, equipos informáticos, redes de comunicación, soportes de información, equipamiento auxiliar e instalaciones físicas involucrados en las actividades de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

De las definiciones: Para los fines de las presentes Políticas se entenderá por:

Servicios: Procesos que la Secretaría que ofrece al exterior o de forma interna, como puede ser el servicio de conectividad a internet, soporte técnico, correo electrónico, análisis y bloqueo de sitios web no permitidos, mesa de ayuda etc.

Datos e información: La información y los datos que se utilizan dentro de la Secretaría para su correcto funcionamiento.

Equipos informáticos: Son todos los dispositivos que se conectan a internet conformando un espacio de trabajo.

Redes de comunicación: Son las encargadas proveer los servicios necesarios para la transacción de información.

Soportes de información: Los soportes físicos permiten el almacenamiento de la información durante un largo periodo de tiempo.

Equipamiento auxiliar: Permite dar soporte a los sistemas de información, estos equipamientos no se incluyen en ninguno de los otros grupos. Un ejemplo de estos es: máquinas de destrucción de documentos, equipos de climatización, impresoras, escáneres y equipos de respaldo de energía.

Instalaciones: Son los lugares físicos donde se alojan los sistemas de información, oficinas u otros.

Activo de Información: Información o medio de procesamiento de información; el cual es de valor o interés para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción y necesita ser protegido correctamente.

Aplicación: es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo.

Obligación: aquella que se debe realizar para preservar la confidencialidad, integridad y disponibilidad de la información. Sanción: castigo que se da al que no cumple una norma establecida o tiene un comportamiento incorrecto.

PDE: La Plataforma Digital Estatal que administra la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

Equipo servidor: Equipo de cómputo diseñado específicamente para el procesamiento de información, recibe peticiones de otros equipos conectados a la misma red y se encarga de responder a esas peticiones dependiendo de la función, en algunos casos puede ser peticiones con el fin de mostrar información o datos.

Secretaría Ejecutiva: De conformidad con el artículo 24 y segundo transitorio, último párrafo, de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo, la Secretaría Ejecutiva del Sistema Estatal es un organismo público, descentralizado, con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión; y además se previene que debe contar con una estructura operativa para la realización de sus atribuciones, objetivos y fines.

DSTyPD: Dirección de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

Usuarios. Las personas servidoras públicas de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción

ISO/IEC 27001: 2013 Information Technology - Security Techniques - Information Security Management Systems – Requirements.

Es una norma internacional que permite el aseguramiento, confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, permite a las organizaciones la evaluación del riesgo y la aplicación de controles necesarios para mitigarlos o eliminarlos.

De las políticas: Para asegurar la confidencialidad, integridad y disponibilidad de la información y activos de información de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción se implementarán las siguientes políticas:

Primera. Responsabilidad

a) Secretaria Técnica.
b) Departamento de Servicios Tecnológicos y Plataforma Digital.
c) Personas servidoras públicas que tengan bajo resguardo o préstamo un equipo de cómputo.

Segunda. Para el uso de las PCs y Laptops:

a) Todo usuario de equipos de cómputo, laptops, servidores, entre otros, propiedad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción es responsable de informar al Departamento de Servicios Tecnológicos y Plataforma Digital la aparición de alguna notificación referente a la actualización y vigencia de su antivirus.

b) Al detectar una actividad maliciosa en las redes institucionales, el servicio al dispositivo o equipo detectado puede ser bloqueado como medida preventiva para asegurar la continuidad de las actividades docentes, de investigación o cumplimiento de las funciones de valor o interés institucional.

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

Tercera. Para el uso de Internet / Intranet:

a) El servicio de internet debe ser utilizado sólo para fines laborales, de investigación o cumplimiento de las funciones y atribuciones de su cargo.
b) Cualquier abuso demostrable con evidencia objetiva sobre la utilización del recurso de internet/intranet será sujeto a sanciones conforme al marco legal de la Ley de Responsabilidades Administrativas para el Estado de Michoacán De Ocampo.
c) Con la intención de optimizar el uso de recursos el usuario debe:
    I. Privilegiar el uso de red cableada a la inalámbrica.
    II. En caso de contingencia se privilegiará la continuidad del servicio de internet sobre el servicio de wifi.

Cuarta. Aplicaciones

a) La instalación de aplicaciones informáticas debe estar justificada por las actividades laborales, de investigación o cumplimiento de las atribuciones a su cargo (ver anexo 2).
b) Se debe contar con las licencias de las aplicaciones instaladas o de lo contrario solicitarlas vía requisición a la Delegación Administrativa.
c) El software libre no deberá poner en riesgo la integridad, disponibilidad o confidencialidad de la información, medios de procesamiento, almacenamiento o transmisión de información.
d) No dejar sesiones abiertas cuya información sea de valor o interés institucional.

Quinta. Físico

a) Para limpieza superficial de los equipos de cómputo no debe utilizar solventes, detergentes u otros medios de limpieza general.
b) Mantener documentación o medios removibles bajo acceso controlado.
c) No consumir alimentos o líquidos en áreas o distancias que puedan dañar documentos, equipos, medios de almacenamiento o procesamiento de información de valor o interés institucional.
d) No mantener peceras, floreros, plantas o cualquier otro que signifique derramamiento de líquidos que pueda dañar documentos, equipos, medios de almacenamiento o procesamiento de información de valor o interés institucional.

Sexta. Acceso a PCs y laptops

a) Se debe activar sesiones de usuarios asegurando que el acceso sea por medio de: usuario / contraseña.
b) No utilizar la opción "recordar contraseña" en el acceso de aplicaciones, PCs, laptops, correo, entre otros.

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

Octava Uso de contraseñas

a) La contraseña debe incluir letras, números y caracteres especiales (símbolos), mínimo de 8 caracteres.
a) No debe incluir nombre o siglas de la dependencia, iniciales o nombre del usuario, nombre del puesto, fecha de nacimiento, número de teléfono, números o letras consecutivas.
b) No se debe compartir contraseñas personales, ni mantener visible las contraseñas. Para más recomendaciones de contraseña segura (ver anexo 3).

Novena. Equipo desatendido y pantalla limpia

a) Se debe bloquear cualquier equipo desatendido con contraseña y mantener bloqueo automático.
b) No guardar documentos o archivos de valor o interés institucional en el escritorio del equipo (pantalla).

Decima. Correo electrónico

Cualquier información o documentación relacionada con las actividades de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, deberá ser enviada por el correo institucional y evitar el uso para estos fines de otros servicios de correo electrónico.

Decima primera. Mensajería (Messenger, FB, Gtalk, entre otros).

No se deberá compartir información confidencial o temas sensibles por este tipo de medios.

Decima segunda. Transferencia de información

a) El envío de información deberá ser por medios seguros como:
   I. Correo institucional
   II. Entrega personal
   III. Documentación impresa confidencial protegida en sobres o folders

Decima tercera. Medios móviles o removibles

a) La información confidencial y restringida de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, no deberá ser almacenada en medios móviles o removibles personales.
b) Las memorias flash (USB, SD, Memory Stick, Micro SD, entre otras) se deberán emplear sólo para la transferencia de datos y no como dispositivos de almacenamiento, la información transferida deberá ser eliminada.

c) Discos externos deberán mantenerse protegidos de acceso no autorizado, evitar estar a la vista y protegerse por contraseña.
d) En el caso de medios de almacenamiento ópticos (DVD, CD, DD externos entre otros) deberá asegurarse su protección contra la humedad, acceso no autorizado, identificación apropiada y al término de su uso la eliminación adecuada.

Decima cuarta. Eliminación segura y reasignación del equipo

En caso de baja/reasignación de equipo, la Secretaría Ejecutiva del Sistema Estatal Anticorrupción deberá atender lo siguiente:

a) El Departamento de Servicios Tecnológicos y Plataforma Digital es el encargado de respaldar y eliminar la información y software con licenciamiento institucional del medio del que se va a disponer.
b) El departamento de Servicios Tecnológicos y Plataforma Digital notifica a Delegación Administrativa la baja o reasignación del equipo.
c) Asegurarse de que la información que se elimine sea de forma segura (Ver anexo 4).

Decima quinta. Proceso Disciplinario

a) En caso de incumplir cualquier disposición definida en las secciones anteriores estarán sujetos a sanciones y medidas disciplinarias según los establecido en el Estatuto Orgánico y ley de Responsabilidades Administrativas para el estado de Michoacán de Ocampo.
b) A todo usuario que incumpla lo señalado en la política de buenas prácticas de usuario, le será notificado vía oficio su incumplimiento por la instancia competente conforme a la normativa aplicable, misma que determinará las acciones pertinentes para resarcir dicha falla.
c) Los asuntos y/o sanciones no contempladas en esta política serán tratados por la Delegación Administrativa de la Ejecutiva del Sistema Estatal Anticorrupción.

Decima sexta. Anexos

a) Anexo 1 "Reporte de monitoreo"
b) Anexo 2 "Solicitud de instalación de aplicación"
c) Anexo 3 "Contraseña Segura"
d) Anexo 4 "Eliminación segura de información"

La revisión y verificación del cumplimiento de la Política de buenas prácticas de usuarios de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, debe ser realizada en el primer semestre del año mediante un registro denominado "Reporte de monitoreo" (ver anexo 1).

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

ANEXO 1

REPORTE DE MONITOREO

Dependencia:		**Fecha de Elaboración**
Proceso:		

ACTIVO	CONTROL	CUMPLIMIENTO		OBSERVACIONES
		SI	NO	
PCs y Laptops	El acceso a través de un usuario y contraseña			
	La contraseña debe incluir letras y números, mínimo 8 caracteres			
	No utilizar la opción "recordar contraseña"			
	Revisar existencia, actualización y vigencia de antivirus			
	Bloqueo inmediato del equipo al detectar una actividad maliciosa en las redes institucionales			
Internet / Intranet	Sólo para fines y cumplimiento de actividades institucionales			
	Privilegiar el uso de red cableada a la inalámbrica			
	En caso de contingencia se privilegia el servicio a funciones de gestión institucional			
Aplicaciones	Sólo para el cumplimiento de las funciones de interés institucional			

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

	Se deben contar con licencias de las aplicaciones instaladas			
	El software libre no deberá poner en riesgo la integridad, disponibilidad o confidencialidad de la información y sus medios			
	No dejar sesiones abiertas en aspectos de interés institucional			
Físico	No colocar medios/equipos de procesamiento de información directamente en el piso			
	Para limpieza del equipo de cómputo debe ser desenergizado y usar el material adecuado.			
Equipo y pantalla limpia	No mantener acceso directo a documentos y/o archivos de interés institucional			
Escritorio limpio	Mantener documentación o medios removibles bajo acceso controlado			
	No consumir alimentos y bebidas en áreas o distancias que puedan dañar cualquier tipo de información.			
	No mantener cualquier objeto que signifique derramamiento o daño de algún tipo o medio de información.			
Correo electrónico	Cualquier información relacionada a las funciones universitarias deberá hacerse sólo por el correo UCOL			
Mensajería	No se deberá compartir información confidencial o temas sensibles a la institución			
Transferencia de información	Sólo por medios seguros			

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

Medios móviles o removibles	Información confidencial no debe ser almacenada en medios móviles o removibles personales			
	Las memorias flash se deberán emplear sólo para transferencia de datos y no como dispositivos de almacenamiento			
	Los discos externos deben ser protegidos de acceso no autorizado y uso de contraseña			
	En medios de almacenamientos ópticos debe usarse protección para humedad y acceso no autorizado			
Uso de cómputo móvil	No sacar el equipo de las instalaciones universitarias para actividades ajenas a las funciones laborales			
	No dejar a la vista el equipo en autos, lugares públicos, etc.			
	No se debe exponer a factores ambientales			

Responsable de Revisión:
Nombre

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

ANEXO 2

SOLICITUD DE INSTALACIÓN DE APLICACIONES

INFORMACIÓN DEL SERVIDOR PÚBLICO			
Nombre:		**Fecha:**	
Cargo:			
Área de adscripción:			
APLICACIÓN SOLICITADA:			
Aplicación solicitada:	Ej. Suite Adobe Creative Cloud	**¿Qué uso se le dará a la Aplicación?**	
Equipo para el cual solicita la instalación:	Ej. SESEA-18		
¿La Aplicación es de uso libre o comercial?	Ej. Uso libre		

*Para la instalación de Aplicaciones de uso comercial, deberán ser requisitadas a la Delegación Administrativa para su adquisición, una vez adquiridas se procederá a la instalación conforme a las políticas de uso del proveedor. En caso de que la Aplicación esté sujeta a temporalidad, el usuario deberá notificar a este Departamento y a la Delegación Administrativa la fecha de expiración y, si es el caso, realizar la solicitud de renovación.

Nombre y Firma del Solicitante	**Vo. Bo. Servicios Tecnológicos y Plataforma Digital**	**Vo. Bo. Lic. Ana María Vargas Vélez, Secretaría Técnica**

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

ANEXO 3

CONTRASEÑA SEGURA

¿Qué es una contraseña segura?

Para que su contraseña se considere segura debe cumplir con los siguientes requisitos:

- Ser privada (Sólo la conoces tú)
- Ser secreta (No guardes tus contraseñas en un lugar público y al alcance de los demás)
- Fácil de recordar (No debe ser necesario escribirla para tenerla en mente)
- No debe ser fácil de adivinar: evita contraseñas que contengan palabras existentes en algún idioma, por ejemplo: Aguilanegra (uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en el diccionario y/o palabras de uso común).
- No uses la misma contraseña para todas las cuentas que establezcas en línea. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.

Recomendaciones para tomar en cuanta durante la creación de una contraseña segura:

- Crea contraseñas que tengan al menos 8 caracteres y combinen letras, números y símbolos.
- No uses palabras reales, aunque estén escritas al revés. Las pueden averiguar en cuestión de segundos.
- No incluyas datos obvios como tu nombre, fecha de nacimiento, el nombre de tu conyugue, hijos, o mascotas.
- Las contraseñas más usadas son patrones de teclado (por ejemplo: qwerty, asdfgh, 123456, etc), nombres propios de personas, palabras malsonantes y "contraseña". Evita el uso de alguna de ellas.
- Evita el reciclado de contraseñas, si lo haces y una de tus cuentas se ve comprometida, todas tus cuentas están en riesgo.

Hay muchas formas de crear contraseñas únicas y complejas que además son fáciles de recordar. Empieza por pensar una frase memorable, por ejemplo, una canción o tu poema preferido. Luego usa la primera letra de cada palabra para crearla. Este puede ser el punto de partida para cada contraseña que crees. Luego, puedes seguir estos simples pasos para mezclarlo un poco, por ejemplo:

- Introduce una mayúscula en algunos de los caracteres.
- Introduce el nombre de la cuenta en la que te estás registrando tras el segundo carácter.
- Introduce un número o reemplaza un carácter alfabético por un número.
- Introduce un símbolo (carácter especial).

Nombre de la Política	Fecha de implantación	Edición	Clave	Fecha de revisión
Políticas para el uso de los equipos informáticos, internet, programas electrónicos y unidades de almacenamiento de la SESEA	01 de abril del 2022	01	SESEA-POL-DSTyPD-01	

Ejemplo práctico:

Vamos a suponer que usamos este refrán como punto de partida: **"Más vale pájaro en mano que cientos volando"** para crear una contraseña segura.

Partiríamos de: **mvpemqcv** y después de seguir los pasos para mezclarlos podría quedar:

+vP3mQcv

De esta manera, tenemos una contraseña segura y fácil de recordar. No olvides que este supuesto es sólo un ejemplo, también puedes hacer uso de **sitios en línea para generar contraseñas seguras (https://www.lastpass.com/es/features/password-generator)**

Ten siempre en cuenta que las contraseñas suponen la primera línea de defensa en la protección de nuestra vida digital. Por lo que debes asegurarte de utilizar el mejor método de protección posible.

Símbolos permitidos (caracteres especiales):

@	[		]	^	_	!
"	#	$	%	&	'	(
)	*	+	,	-	.	/
:	;	{	}	<	>	=
|	~	?	A-Z	a-z	0-9	

ANEXO 4

ELIMINACIÓN SEGURA DE INFORMACIÓN

Antes de proceder:

Se debe identificar la información que es de valor para esta Secretaría, luego de identificar la información se procederá a la realización del respaldo en un medio o dispositivo para tal fin, y que cuente con suficiente espacio, tales como CD, Disco Duro externo, DVD, tarjetas de memoria SDCARD, USB o algún espacio en la nube.

El software eliminará toda la información contenida en los discos duros de la computadora (lógicos y físicos), así como cualquier disco duro externo, memoria USB o disco flexible que se encuentre conectado al equipo de cómputo.

Una vez eliminada, no será posible recuperar la información que se encuentre en los dispositivos mencionados. Se recomienda revisar la información del equipo de cómputo las veces que sea necesario, asegurándose de no eliminar datos sin respaldar.

Procedimiento:

1. Asegurarse de haber realizado el respaldo de la información que represente valor para la Secretaría, previamente identificado en el medio o dispositivo usado, se puede verificar consultando el medio o dispositivo en algún otro equipo de cómputo.
2. Elegir cómo se va a eliminar la información:
   a. Eliminar archivos específicos de forma **permanente**
      i. Localizar los archivos que se desean eliminar
      ii. Seleccionar 1 archivo
      iii. Seleccionado el archivo, pulsar la tecla **Mayús**, seguida por la tecla **Supr**
      iv. Repetir el procedimiento hasta eliminar todos los archivos deseados
   b. Restaurar el equipo de cómputo a los **valores de fábrica**
      i. Desconectar todos los dispositivos y medios de almacenamiento del equipo
      ii. Abrir el panel de **Configuración** (Se accede haciendo click en Inicio, luego en Configuración)
      iii. Acceder al módulo **Actualizar y seguridad**
      iv. Dar click en la opción **Recuperación**, y dar click en el botón Comenzar de la opción *Reestablecer este equipo.* Se abrirá una ventana de diálogo.
      v. En la ventana de diálogo, elegir la opción **Quitar todo**, se iniciará un asistente que le guiará en el proceso de restauración.